UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

HISCOX INSURANCE COMPANY INC. and HISCOX SYNDICATES LIMITED	)	
	)	Case No. 4:20-cv-00237-NKL
Plaintiffs,	)	
vs.	)	
WARDEN GRIER, LLP	)	
Defendant.	)	

WARDEN GRIER, LLP'S SUGGESTIONS IN SUPPORT FOR ITS MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes and Rules

Other Authority

INTRODUCTION

On February 14, 2017, the attorneys at Warden Grier received an email from an international criminal organization calling itself "The Dark Overlord" (TDO). In this email, TDO informed Warden Grier it had collected a significant number of documents from the law firm's server. TDO threatened to release these documents on the Internet unless Warden Grier paid 50 Bitcoin in ransom and did not make the fact of the hack known. If Warden Grier paid the ransom, TDO would destroy the documents it had taken.

Immediately, Warden Grier reached out to their IT vendor to secure their network. They also engaged the services of a data breach attorney who put them in touch with a forensic IT vendor. The forensic examiner took an image of the server to determine what data may have been exfiltrated by TDO and how the hack occurred. The forensic examiner verified that the firm's system had been breached in December 2016, but the hackers had covered their tracks forensically and no one could be sure exactly what data had been accessed or acquired by TDO.

Warden Grier also engaged in discussions with Jeff Jensen, a white-collar defense attorney, and Chris Budke, a former FBI agent, to learn more about TDO from the FBI.[1] The FBI was aware of 24 known instances of the TDO extortion due to cyber theft and the 23 victims who did not pay the ransom had their data released on the Internet by TDO.[2] The one victim that paid the ransom did not have its data released. After considering all the potential outcomes, Warden Grier determined that the best way to protect its clients' data was to pay the ransom out of their own pocket. TDO confirmed receipt of the ransom and that the documents had been deleted.

---

[1] Jeff Jensen subsequently became the U.S. Attorney for the Eastern District of Missouri and was instrumental in the extradition of a TDO member from England for prosecution in St. Louis, Missouri.

[2] One of the victims who did not pay TDO was Netflix and TDO released a season of "Orange is the New Black" on the internet prior to its Netflix release.

In 2018, another hacker group claiming to be TDO contacted Warden Grier again and sought an additional ransom for "notes" they claimed they had discovered which had not been deleted. The communications from this group became threatening, even involving a death threat to Mike Grier. As Warden Grier was working with the FBI to determine if this new threat was legitimate – or if the hackers still had any client documents – the hackers contacted one of Warden Grier's clients, Hiscox, on March 30, 2018. Hiscox then contacted Warden Grier to confirm the hack had occurred and immediately demanded that Warden Grier turn over Hiscox-related data from its server. Hiscox needed the data to determine its own legal obligations now that it was aware of the breach. Warden Grier cooperated with Hiscox by hiring Control Risks Group (CRG), a third-party vendor specified by Hiscox, to collect and cull the Hiscox-related data from the server and provided a list of all Hiscox policyholders that may have had data on the server.

Hiscox hired Cooley, a data breach law firm, which coordinated the analysis of the Hiscox-related data by Charles River Associates (CRA), also hired by Hiscox. Hiscox also engaged a public relations firm, Brunswick, to assist with media releases and notification templates and another vendor, Epiq, to handle the notification process. Hiscox ultimately decided to only notify its policyholders – and not a single individual – about the data breach, leaving any individual notifications up to its client policyholders.

Hiscox now alleges it incurred over $1.5 million in this process and seeks to be reimbursed for its costs from Warden Grier. But Hiscox has no legal basis for recovering its costs from Warden Grier, Hiscox's claims fail as a matter of law and Warden Grier respectfully requests summary judgment be entered in its favor.

KEY INDIVIDUALS AND GLOSSARY OF TERMS

Individuals Cited to in Suggestions in Support

Ben Walter	CEO of Hiscox USA
Jeremy Pinchin	Hiscox Head of Claims
Hanna Kam	Hiscox Group Chief Risk Officer
Tara Bodden	Hiscox Senior Vice President Claims, Media & Technology
David Schonbrun	Hiscox USA Head of Legal and Government Affairs
Amy Yung	Hiscox Associate Counsel, Complex Claims Specialist
Cooley LLP	Global Law Firm
David Navetta	Partner at Cooley LLP
Amy Reeder Worley	Berkeley Research Group, Hiscox retained expert
Control Risk Group (CRG)	Obtained Hiscox data from Warden Grier
Charles River Associates (CRA)	Analyzed Hiscox data obtained from CRG
Brunswick Group, LLP	Public Relations and Communications firm
EPIQ Systems	Legal service and support company

Key Terms Used in Suggestions in Support

PII	Personally Identifiable Information
NPPI	Non-public Personal Information
TDO	The Dark Overlord
Policyholders/Insureds	NOTE: These terms are used interchangeably and refer to the commercial entities insured by Hiscox (also referred to as Hiscox's "customers")

ARGUMENT

This case has been narrowed to two discrete claims against Warden Grier: (1) breach of fiduciary duty and (2) negligence for failing to adequately investigate and advise Hiscox of the data breach. However, Warden Grier did not breach its fiduciary duty to Hiscox by not notifying Hiscox of the data breach in 2017. And Warden Grier was not negligent for failing to comply with the Missouri data breach statute or any other states' data breach statutes. In short, both tort claims fail because Warden Grier did not breach any duties it owed to Hiscox.

Furthermore, Hiscox cannot prove an injury or damages as required under Missouri law and, therefore, cannot meet their burden of proof. Hiscox is essentially seeking indemnification from Warden Grier for the costs Hiscox voluntarily incurred to meet its own legal duties and there is no basis for Hiscox to seek indemnification for those costs. The undisputed facts demonstrate that the breach of fiduciary duty and negligence claims fail as a matter of law and the Court should grant summary judgment in favor of Warden Grier.

I. The only remaining claims are Breach of Fiduciary Duty and Negligence.

Hiscox has dropped its contract claims. Statement of Facts ("SOF") 4. For the two remaining tort theories, Hiscox asserts that Warden Grier breached its fiduciary and statutory duties to Hiscox by (1) failing to protect personal information; (2) failing to adequately investigate the 2016 Data Breach; and (3) failing to advise Hiscox that its "PI" had been compromised.

1. Failing to Protect Personal Information

Hiscox has dropped its contract claims completely and revised its breach of fiduciary duty and negligence claims to no longer claim that Warden Grier was responsible for "allowing the data breach to occur or in its data security practices, policies, or procedures." SOF 4. Therefore, this

alleged failure has been dropped from this case, along with both contract claims in their entirety.[3]

2. Failing to Adequately Investigate the 2016 Data Breach

The basis of the claim that Warden Grier failed to adequately investigate the 2016 Data Breach is that Warden Grier failed "to hire a forensic IT firm to investigate the 2016 Data Breach or, if it did, has refused to provide Hiscox with the findings of any such investigation." *Complaint*, ¶ 12. Hiscox alleges that because Warden Grier failed to conduct a forensic investigation, or refused to share findings of such, Hiscox commenced its own investigation. *Complaint*, ¶ 20. The emphasis is on a forensic investigation in the Complaint, but there is undisputed evidence that Warden Grier investigated the data breach, including a forensic investigation.

On February 15, 2017, Warden Grier hired David Chronister, a forensic expert with Parameter Security, a forensic IT firm, to investigate the 2016 Data Breach. SOF 11. Chronister worked in the Warden Grier offices, imaging and analyzing the servers and computers. SOF 20. On February 17, 2017, Chronister reported that someone had gained access to the firm's servers, removed copies of data from the servers, covered their tracks, and deleted logs. SOF 20. On February 19, 2017, Chronister sent Warden Grier a list of files from the server to review. SOF 5. Warden Grier also had a detailed sense of the type of information on the server. SOF. 5.

After Hiscox learned of the data breach in 2018, Warden Grier told Hiscox of the investigation in 2017. SOF 29. In cooperating with Hiscox, Warden Grier also provided a copy of the forensic image of the server taken by Parameter (in 2017) to the third-party vendor hired to isolate the Hiscox-related data on the server. SOF 44. Hiscox has offered no evidence and no expert opinion that the forensic investigation by Warden Grier was inadequate.

[3] In data breach cases across the board, the foundation for the claims asserted by plaintiffs is that the breached entity failed to protect the data. Dropping all claims related to Warden Grier being responsible for the data breach should be fatal to the merits of the remaining claims.

3. Failing to Advise Hiscox that its "PI" had been compromised

Hiscox defines "PI" as "highly sensitive, confidential, and proprietary information, including protected health and personally identifiable information belonging to Hiscox and/or Hiscox's insureds." *Complaint*, ¶ 9. But as commercial entities, neither Hiscox nor its insureds have protected health or personally identifiable information ("PII"). SOF 7, 8, & 9. There is undisputed evidence that Hiscox was advised of the data breach in 2018 (SOF 29) and Hiscox was aware that a limited amount of individual PI was in the Hiscox-related data. SOF 6.

Hiscox has also not identified any specific damages tied to the delay between Warden Grier learning of the data breach in 2017 and Hiscox being informed of the data breach in 2018. SOF 30. Key individuals at Hiscox have indicated they would have undertaken the same analysis of the Hiscox-related data in 2017 as they did in 2018. SOF 30, 31. If Hiscox did not suffer any additional damages due to the delay between Warden Grier learning of the data breach in 2017 and Hiscox learning of the breach in 2018, then any claim by Hiscox that Warden Grier breached its duties to advise Hiscox of the breach during that 15-month period fails as a matter of law. *See Hiers v. Lemley*, 834 S.W.2d 729, 733 (Mo. 1992) (no recovery available when there are no damages despite alleged delay in informing patient of erroneous diagnosis); *see also McCrary v. Missouri, K. & T. Ry. Co.*, 99 Mo. App. 518, 74 S.W. 2, 3 (1903) (there can be no damages for mere delay).

II. Warden Grier did not breach any fiduciary duties to Hiscox.

1. No fiduciary duty existed if Warden Grier is equivalent to a data storage provider.

Hiscox has taken the position that it is not suing Warden Grier in its capacity as attorneys for Hiscox. Rather, Hiscox has stated on the record that "Plaintiffs' claims do not actually arise out of Defendant's provision of legal services, and instead arise from the more mundane area of Defendant's data security practices and Defendant's willful decision to not notify its clients,

including Plaintiffs, when their data was compromised." [Doc. 16].

But if Warden Grier is deemed to be a data storage provider, then there is no fiduciary relationship. A fiduciary relationship is not created just because one party is in possession of non-public information. *See Citizens Bank of Pennsylvania v. Reimbursement Techs., Inc.*, 609 Fed. Appx. 88, 94 (3d Cir. 2015) (citing *Dirks v. SEC*, 463 U.S. 646, 654, 103 S.Ct. 3255, 77 L.Ed.2d 911 (1983)); *see also Bunzl Distribution USA, Inc. v. Schultz*, 4:05CV605 JCH, 2006 WL 3694634, at *3 (E.D. Mo. Dec. 13, 2006) ("The existence of a business relationship does not, in itself, give rise to a fiduciary relationship."). Because there is no fiduciary duty between a data provider and a data owner, this claim must fail as a matter of law.

2. Warden Grier did not violate its duties of client loyalty or confidentiality to Hiscox.

If Hiscox is now arguing that a fiduciary relationship exists based on the attorney-client relationship, the elements of a fiduciary duty claim are: "(1) an attorney-client relationship; (2) breach of a fiduciary obligation by the attorney; (3) proximate causation; (4) damages to the client; [and] (5) no other recognized tort encompasses the facts alleged." *Klemme v. Best*, 941 S.W.2d 493, 496 (Mo. 1997). In the attorney-client relationship, this requires a showing that "the attorney violated the duty of client loyalty or the duty of confidentiality." *Costa v. Allen,* 274 S.W.3d 461, 462 (Mo. 2008). When attorneys demonstrate loyalty to their clients, seek to protect the confidentiality of client communications and place their clients' interests above their own, then there can be no breach of the fiduciary duty. *See Salau v. Jones*, 2:14-CV-04307-NKL, 2015 WL 5999781, at *4 (W.D. Mo. Oct. 13, 2015). Hiscox has abandoned its claim that Warden Grier failed to protect confidential information by allowing the data breach to occur or in its data security practices, policies or procedures (SOF 4) leaving only a claim that Warden Grier breached an ethical duty in failing to advise Hiscox of the breach.

The ethical duties for Warden Grier are expressed in the Missouri Rules of Professional conduct, which "have the force and effect of judicial decision." *McVeigh v. Fleming*, 410 SW 3rd 287, 289 (Mo.E.D. 2013). Hiscox's own data breach counsel agrees there is nothing in the Missouri Rules of Professional Conduct requiring a duty to notify clients of a data breach.[4] Under the Missouri rules, regarding the dissemination of confidential information, attorneys are obligated to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client." M.R.P.C. 4-1.6(c). The Missouri rules recognize that "many difficult issues of professional discretion can arise. Such issues must be resolved through the exercise of sensitive professional and moral judgment guided by the basic principles underlying the Rules." M.R.P.C. Preamble, ¶ 9. And "in some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication." M.R.P.C. 4-1.4, cmt. 6. When considering the discipline of attorneys, Missouri Supreme Court Rule 4 states that the "Rules presuppose that disciplinary assessment of a lawyer's conduct will be made on the basis of the facts and circumstances as they existed at the time of the conduct in question and in recognition of the fact that a lawyer often has to act upon uncertain or incomplete evidence of the situation."

Warden Grier took reasonable measures to keep its clients' confidential data – including the Hiscox-related data – from being disseminated in 2017. Warden Grier undertook extensive measures to understand the nature of the data breach and the implications of the breach being

[4] David Navetta, a Partner at Cooley, the law firm hired by Hiscox to assess its legal obligations, advised Hiscox that that the Rules of Professional conduct "do not require any notification following a breach [but] they do require lawyers generally to act in an ethical manner and zealously represent their clients." He went on to point out that confidentiality provisions and notification requirements following a security incident can be handled by client agreements. SOF 22.

accomplished by an international hacking organization. Warden Grier specifically:

- Contacted data breach counsel Peter Sloan (SOF 10);
- Had Cytek, its IT vendor, and forensic expert Parameter Security review systems and the nature of breach (SOF 11);
- Understood the information on the server (SOF 5);
- Engaged in conversations with attorney Jensen who was familiar with white collar crimes (SOF 12); and
- Engaged in conversations with FBI about the known behaviors of TDO (SOF 13).

Warden Grier weighed all the information obtained from these experienced sources against the threats and *quid pro quo* statements of TDO to determine the best possible manner for keeping client data from being made public. TDO threatened to release data unless the ransom of 50 bitcoin was paid and no one was told. SOF 14, 16 & 19. On the other hand, TDO promised to destroy the data if ransom was paid. SOF 19. And the FBI had experience with TDO when ransom was not paid (data released) and when ransom was paid (data not released). SOF 15.

When faced with whether to disclose information about the breach to its clients in 2017, Warden Grier weighed its ethical and legal obligations and determined that notifying the clients would only harm its clients, while paying the ransom was the most likely way to protect its clients. Thus, Warden Grier paid the ransom from its own funds as the best means to protect the confidentiality of is clients' data. SOF 16. Warden Grier also documented its analysis, evaluation of the risks, and reasons for its decisions to pay the ransom and not notify clients at that time. SOF 20, *Memorandum*. Peter Sloan, data breach counsel for Warden Grier, has testified that "Warden Grier's decision on the handling of the circumstances of this event between the spring of 2017 and March 2018 in my view was appropriate." SOF 21.

In fact, Hiscox has agreed that the measures taken by Warden Grier in 2017 likely prevented the public disclosure of the information that had been stolen from the Warden Grier

server. SOF 24.[5] Hiscox's own expert testified that when Warden Grier paid the ransom to TDO, it was part of its obligation to protect clients and it was in the clients' interest to have the information in the hands of TDO destroyed. SOF 17, 18; *Complaint*, ¶ 15 ("Warden Grier paid the Hackers a ransom or other demand to protect its and its clients' personal information from dissemination.").

In essence, there was a real threat its clients' data would be disclosed if Warden Grier made the fact of the hack public through client notifications, so Warden Grier remained loyal to its clients, collectively, by taking measures to protect the clients' confidential data from being disseminated in 2017. Accordingly, Warden Grier did not breach its fiduciary duties to Hiscox by failing to advise Hiscox of the data breach after Warden Grier learned of the hack in 2017.

III. Warden Grier was not negligent for failing to notify Hiscox based on any duty created by data breach statutes.

Hiscox has dropped the contract claims and the common law (fiduciary duty) claim has been discussed above. The remainder of Hiscox's negligence claim is that Warden Grier breached statutory requirements "to notify Hiscox and other firm clients (including Hiscox-insured clients)" of the data breach. *Complaint*, ¶ 46 (emphasis added). Whether an entity has breached a duty through its negligence is typically a matter of fact to be determined by the jury. *Luallen v. Reid*, 58 S.W.3d 50, 53 (Mo.App. W.D. 2001). However, the question of whether a legal duty exists to begin with is "a question of law to be decided by the court." *Strickland v. Taco Bell Corp.*, 849 S.W.2d 127, 131 (Mo.App. E.D. 1993). The duty can arise from one of three sources: "(1) the legislature; (2) the common law; or (3) by contractual agreement." *Midwest Bankcentre v. Old Republic Title Co. of St. Louis*, 247 S.W.3d 116, 123 (Mo.App. E.D. 2008).

[5] Hiscox has in other situations, for its cyber insurance policyholders, agreed to pay a ransom for the insured to have the insured's information returned or destroyed by the hacker. SOF 23.

1. Hiscox cannot assert a claim under the Missouri data breach statute.

In its Complaint, Hiscox specifically alleges Warden Grier failed to comply with the Missouri data breach statute. *Complaint*, ¶ 47.[6] But although Hiscox has alleged a breach of Missouri's data breach statute, this statute does not allow for a private cause of action. *See* R.S.Mo. § 407.1500.4 ("The attorney general shall have exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section."). The Missouri Attorney General "has exclusive authority in bringing claims against data handlers for a violation of the notice requirements." *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1056 (E.D. Mo. 2009). "A federal court must ask 'whether the constitutional or statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief.'" *Glickert v. Loop Trolley Transp. Dev. Dist.*, 792 F.3d 876, 881 (8th Cir. 2015) (internal quotation omitted).[7]

Furthermore, notices required by the Missouri data breach statute are to be "provided to affected consumers." R.S.Mo. § 407.1500.2(6) (emphasis added). "Consumer" is defined by the statute as: "an individual who is a resident of this state." R.S.Mo. §407.1500.1(2). Hiscox is not a "consumer" as defined by the statute as it is (1) not an individual and (2) not a "resident" of Missouri. SOF 2a. Therefore, the notice requirements in R.S.Mo. § 407.1500.2(4) regarding

[6] As plead and as testified to by the retained expert for Hiscox, this now appears to be a negligence *per se* claim. Under Missouri law, "'the doctrine of negligence *per se* has traditionally arisen in cases involving personal injury and physical injury to property[,]" and the doctrine had not yet been extended to any case that involved damage to economic interests." *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 762 (C.D. Ill. 2020) (refusing to find negligence *per se* for violation of the Missouri data breach statute when plaintiff suffered only economic losses) (quoting *Lowdermilk v. Vescovo Building & Realty Co., Inc.*, 91 S.W.3d 617, 628 (Mo. Ct. App. 2002)).

[7] The *Glickert* court found that plaintiffs in that case did not fall within the persons protected by the Missouri Transportation Development District Act and that plaintiffs were barred from "asserting the rights or legal interests of others in order to obtain relief from injury to themselves." 792 F.3d at 882.

notification to individuals do not apply to Hiscox. Because the Missouri data breach statute does not create a private cause of action and Hiscox is not a protected party under the statute, the negligence claim premised on the Missouri data breach statute must be dismissed.

2. Hiscox can only assert a claim based on negligence by Warden Grier as to Hiscox.

The only issue is whether Warden Grier breached a statutory duty as to Hiscox. Hiscox cannot bring its claims under the entire statutory scheme of data breach statutes across the United States. *See Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1057 (E.D. Mo. 2009) (plaintiff not allowed to bring a claim against a Missouri resident based on data breach statutes of other states "where such a cause of action does not exist under Missouri law.").

Moreover, Hiscox cannot assert a negligence claim based on a generic duty Warden Grier may have had to Warden Grier's other clients, individuals, or Hiscox's insureds. Hiscox must assert its own legal rights and interests and "cannot rest [its] claim to relief on the legal rights or interests of third parties." *The Weitz Co., LLC Mh Metro., LLC v. Brush Creek Realty Fund, LLC*, 12-CV-00738-W-DW, 2013 WL 12130029, at *3 (W.D. Mo. Oct. 8, 2013). "It is not enough to show that the obligation was to another person or class, and that if performed as to them, plaintiff would not have been injured." *Vanacek v. St. Louis Pub. Serv. Co.*, 358 S.W.2d 808, 811 (Mo. 1962).

IV. Hiscox has suffered no injury as a result of the data breach and Hiscox does not have actual damages flowing from any breach of duty by Warden Grier.

1. Hiscox has admitted it did not suffer any injury from the data breach, nor does it anticipate future injury.

Tort theories of negligence and breach of fiduciary duty require a showing of "injury" or "harm." A fiduciary duty claim requires "damages to the client." *Klemme v. Best*, 941 S.W.2d 493, 496 (Mo. 1997). A cause of action for negligence does not arise "until a plaintiff suffers an injury."

Baugher v. Gates Rubber Co., Inc., 863 S.W.2d 905, 913 (Mo.App. E.D. 1993) (emphasis added). In data breach cases, courts will find an injury-in-fact exists when the plaintiff (or class representative) can demonstrate actual harm – such as fraudulent charges, impacts to credit reports, or identify theft – while other courts will find injury-in-fact when there is an increased risk of imminent future harm. *See e.g.*, *In re SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017).[8]

Hiscox has admitted it suffered no injury, and is not likely to suffer a future injury, as a result of this data breach. Hiscox was requested in January 2019 to respond to an inquiry from the New York Division of Financial Services ("NYDFS"). In response to this request, Hiscox sent a letter to the NYDFS stating that "this incident has not materially harmed, and is not reasonably likely to materially harm, any material part of Hiscox's normal operations." SOF 69. That admission is fatal, moreover, it has been over four years since Warden Grier learned of the breach in 2017 and there have been no claims or lawsuits or any indication the data has been misused. SOF 27, 70. Because Hiscox has made a public admission that it has suffered no "material harm" and is not likely to be "materially harmed," then it has suffered no injury (present or imminent) and the breach of fiduciary duty and negligence claims should be dismissed.

2. Hiscox's alleged damages are out-of-pocket expenses and not actual damages under Missouri law.

The alleged "damages" do not qualify as actual damages under Missouri law. Data breach cases tend to be class action lawsuits because they involve the acquisition of personal data, usually financial data, about individuals who transacted business with a commercial entity. In many cases, the plaintiffs (or class representatives) suffered actual harm to their credit ratings, were denied

[8] See also *George D. v. NCS Pearson, Inc. & Pearson Ed., Inc., doing business as Pearson Clinical Assessment*, CV 19-2814 (JRT/KMM), 2020 WL 3642325, at *2 (D. Minn. July 6, 2020) (holding that plaintiff had not suffered an injury-in-fact despite hackers actually acquiring his birthdate).

credit, or even suffered identity theft. In other cases, the evidence is overwhelming that there is an "imminent" threat of future harm (although the courts are split on what types of future harm may provide standing for a plaintiff). But courts have consistently held that the types of costs incurred by Hiscox are not recoverable in data breach cases. *See In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017) (where court held that "costs incurred to mitigate their risk of identity theft, including time [plaintiffs] spent reviewing information about the breach and monitoring their account information" was not recoverable because there was no allegation of a substantial risk of future identify theft); *see also Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416, 133 S.Ct. 1138, 1151 (2013) (plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending").

Furthermore, Missouri is not a state that "envision[s] some type of monetary recovery" in the event of a data breach because Missouri's data privacy statute only has a "consumer-facing mandate" for notice and the state's attorney general has "exclusive authority for enforcing Missouri's data breach notice statute by a civil action." *Cmty. Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 818 (7th Cir. 2018) (analyzing Missouri law).[9]

The alleged "damages" in this case are out-of-pocket expenses incurred by Hiscox to meet its own legal obligations; these kinds of economic losses are not allowed under Missouri law. Hiscox has alleged that it suffered in excess of $1.5 million for significant internal operational losses and costs which include costs to investigate the breach, notify its insureds and make necessary accommodations and to protect affected persons against future harm. *Complaint*, ¶ 22.

[9] The *Cmty. Bank of Trenton* court found that a class of banks could not recover costs such as "employee time to investigate and resolve fraud claims, payments to indemnify customers for fraudulent charges, and lost interest and transaction fees on account of changes in customer card usage," because Missouri's data breach statute did not allow for a private cause of action.

Hiscox has only produced evidence of its damages as invoices for Cooley (legal advice),[10] CRA (data analysis), Brunswick (public relations) and EPIQ (notifications). (SOF 59).

Hiscox has admitted that it suffered no material harm, is not likely to be materially harmed in the future, and its out-of-pocket costs are not tied to any legally recognized injury or harm suffered by Hiscox because of the data breach.

V. Hiscox seeks indemnification for economic costs it incurred to fulfill its own legal obligations, without a contractual or common law basis for indemnification.

1. To be reimbursed for costs Hiscox must demonstrate that the duties Hiscox undertook were identical to those Warden Grier should have undertaken.

There is no allegation by Hiscox of a contractual basis for indemnification. To otherwise be entitled to reimbursement for paying damages which allegedly should have been paid by someone else, "the doctrine of implied indemnity applies only where an identical duty owed by one is discharged by the other. In other words, the doctrine is inapplicable unless the indemnitee and indemnitor have co-extensive, identical duties." *Global Petromarine v. G.T. Sales & Mfg., Inc.*, 577 F.3d 839, 846 (8th Cir. 2009) (internal citations omitted). Tara Bodden testified that as an insurance company, Hiscox is subject to different regulations and has certain legal obligations that are specific to an insurance company that operates in the United States that may be completely different and separate from Warden Grier's obligations after a data breach. SOF 34.

Pinchin testified that Hiscox hired the Cooley law firm because Cooley was "considered to be the best attorneys in the U.S. to provide us with advice as to how to manage this matter and

[10] Under Missouri law, "attorneys' fees are not recognized as consequential damages in the absence of an underlying contract or statute awarding such fees." *Perficient, Inc. v. Munley*, 4:19-CV-01565-JAR, 2021 WL 1427797, at *12 (E.D. Mo. Apr. 15, 2021). *See also*, *Allied Sys., Ltd. v. Teamsters Auto. Transp. Chauffeurs, Demonstrators & Helpers, Local 604, Affiliated with the Int'l Broth. of Teamsters, Chauffeurs, Warehousemen & Helpers of Am.*, 304 F.3d 785, 792–93 (8th Cir. 2002) (fess not allowed as actual damages where claim for attorneys' fees was alleged as an element of damages for legal costs related to stopping a strike.)

ensure at all times complied with the appropriate legal obligations of Hiscox towards any third party, individual or regulators and to the best of my knowledge, we always followed their advice." SOF 37. Cooley had two roles – one, advise CRA what to do with the data and two, advise Hiscox as to their notification requirements. SOF 38.

In determining how to meet its own legal obligations step one for Hiscox was to get the compromised data. SOF 31, 33. Once the data was analyzed by Cooley and Charles River Associates, Hiscox sent out notices to whoever Hiscox believed they were required to by law and informed any regulators Hiscox believed they were obligated to inform. SOF 32. Notes from a Hiscox team meeting on July 20, 2018 reflect a discussion that Hiscox wanted to do what it was legally required to do "and not too much more." The document also reflects Hiscox's thought that "legally our only obligation is to notify them that it happened. Our legal obligation ends when we've notified the customers." According to Yung: "That means that our legal obligation was to notify the customers and nothing more." SOF 55.

As to Warden Grier's obligations, David Navetta, the lead Cooley attorney, testified that Warden Grier "needed to notify Hiscox of the breach. That was their obligation, including providing them enough information for Hiscox to be able to do their own investigation analysis and notice." SOF 39. Warden Grier needed to do a reasonable investigation and cooperate with Hiscox so Hiscox could fulfill their legal obligations. SOF 40. Warden Grier fully cooperated with Hiscox. SOF 42. After Warden Grier confirmed the data breach occurred, "at Hiscox's request, Warden Grier retained Control Risks Group (CRG) to index the Compromised Server, analyze what portion of the data related to Hiscox and provide Hiscox with copies of its data on the Compromised Server. On or around April 4, 2018, Warden Grier provided Hiscox and CRG with a list of Hiscox cases that Warden Grier had handled to aid in the segregation of Hiscox's Client

Data from other Warden Grier clients' data on the Compromised Server." SOF 41. Furthermore, Warden Grier provided CRG with the forensic image of the compromised server that had been made by Parameter in 2017 as well as the list of the Hiscox policyholders.[11] SOF 44, 45.

CRG culled documents from the Warden Grier server as being Hiscox-related data and sent these documents to CRA for Hiscox's review. SOF 43, 46, 62. Hiscox understood that CRG was acting for Warden Grier with respect to culling the Hiscox-related data and that CRA was acting exclusively for Hiscox/Cooley. SOF 61.

2. Hiscox undertook an extensive, expensive, and elective analysis of the data to determine its own legal obligations.

After being informed of the data breach, Hiscox formed a Project Harry Core Group. SOF 35. Knowing it was obligated to investigate what regulatory obligations applied to it and its customers (SOF 67), Hiscox elected to search 1.7 million documents culled from the Warden Grier server to identify individuals with PII. SOF 60, 62. Ultimately, CRA narrowed the documents from 1.7 million to just over 14,000 that may have contained individual names and possible PII. SOF 60, 62. If Hiscox wanted Warden Grier to analyze the data, there is usually a collaborative discussion, as testified to by Hiscox's expert: "I would expect that Hiscox and Warden Grier would be having a discussion about analyzing the data to determine what are the ongoing responsibilities." SOF 63. Hiscox did not request Warden Grier to analyze the data or to pay for Cooley and CRA. SOF 64, 65, 66. Even if Hiscox had asked Warden Grier to conduct the thorough analysis of the Hiscox data, the contracts which established the attorney-client relationship allow for Warden Grier to charge Hiscox to review the Hiscox-related data. SOF 2d, 2e. And to the extent

[11] Warden Grier also utilized ransom and notice specialists recommended by Hiscox, entered into a Common Interest Agreement, and agreed to coordinate its notices to other clients with Hiscox. SOF 47, 48, 49 50.

Hiscox believes Warden Grier's investigation of the data was not adequate, Missouri courts have not recognized a tort of "negligent investigation." *Monroe v. CMMG, Inc.*, 2:15-CV-04172-NKL, 2015 WL 9581853, at*9 (W.D. Mo. Dec. 30, 2015).

After spending over a million dollars on the analysis of the Hiscox documents, over two hundred thousand on legal fees, and one hundred thousand on public relations, Hiscox determined they were not obligated to notify anyone or any regulator and were simply "managing the notification process as a courtesy to our policyholders." SOF 58. Because Cooley determined that Hiscox and Warden Grier were "service providers" with no obligation to notify individuals (SOF 52, 57), Hiscox only notified its insureds. *Complaint*, ¶ 21; SOF 54. Despite Pinchin stating that Hiscox had a legal and moral obligation to notify individuals and "our primary focus was 100 percent ensuring that individuals whose data had been breached were informed of that fact as soon as sensible and achievable" (SOF 36, 51), Hiscox did not notify a single individual. SOF 54. Hiscox left it up to their policyholders to provide individuals with notice. SOF 56. And Hiscox is not aware of any individuals receiving notifications. SOF 72. Any search by Hiscox for individual PII in the data was extraneous and voluntary in that it had no obligations to directly notify any of the individuals in the Hiscox-related information.[12]

Hiscox clearly had different legal duties than Warden Grier. Now Hiscox claims Warden Grier should pay for the costs incurred by Hiscox for its expensive analysis because of its own perceived legal and "moral" obligations. SOF 51. No other client of Warden Grier has done so. SOF 68. There is no contractual, common law, or statutory basis for indemnification. Therefore, the claims asserted by Hiscox against Warden Grier must be dismissed.

[12] Cooley advised that Hiscox may want to notify individuals, and that would be the "right thing to do" but it would be voluntary and expensive.

Dated: September 15, 2021

Respectfully submitted,

/s/ Andrea S. McMurtry

HORN AYLWARD & BANDY, LLC
Robert A. Horn MO #28176
Andrea S. McMurtry MO #62495
2600 Grand Blvd., Suite 1100
Kansas City, MO 64108
Telephone: 816-421-0700
Facsimile: 816-421-0899
rhorn@hab-law.com
amcmurtry@hab-law.com

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that on September 15, 2021, the foregoing was served through the Court's CM/ECF notification system, which will provide service to all counsel of record.

/s/ Andrea S. McMurtry
Attorney for Defendant